1. Introduction

La physique quantique est une branche de la physique théorique qui vise à comprendre le monde à l'échelle microscopique. Elle dispose d'un ensemble des phénomènes et des lois quantiques fondamentalement différents de la plupart de ceux qui semblent s'appliquer à notre propre échelle. Des physiciens, des informaticiens et des mathématiciens ont montré que ces phénomènes, tels qu'ils sont formulés par la mécanique quantique, peuvent être exploités pour représenter et traiter l'information.

Dans ce chapitre, nous dégageons tous les concepts principaux qui nous seront utiles tout au long de ce mémoire. Comme nous sommes confrontés à un domaine complètement nouveau pour un informaticien, nous commençons par la présentation des notions mathématiques adéquates. Nous tentons ensuite d'expliquer les postulats de la mécanique quantique tout en gardant notre point de vue en tant que des informaticiens. Finalement, nous introduisons quelques phénomènes quantiques qui sont à la base du calcul quantique.

2. les préliminaires mathématiques nécessaires

2.1. Espace d'Hilbert

Tout état quantique d'une particule est caractérisé par un vecteur d'état appartenant à l'espace des étatsε, un espace vectoriel appelé « *espace de Hilbert* ». Le vecteur d'état est un vecteur de cet espace qui contient toute l'information sur le système physique étudié. Dans toutes les définitions, le cas d'un « *espace de Hilbert* » indicé par un nombre entier est choisi (espace discret de dimension finie ou infinie) [1].

2.2. Formalisme de Dirac

La notation de Dirac est appeler « *Bra-Ket* » qui permet de représenter l'état du système par un vecteur normé $|\varphi\rangle$ prononcé « *Ket psi* » et $\langle\varphi|$ prononcé « *Bra psi* » [1].

Remarque :

- En anglais, le symbole $\langle \ | \ \rangle$ est appelée « *bracket* » (c'est-à-dire crochet), d'où l'appellation Bra pour la partie gauche et $\langle \ |$, et ket pour la partie droite $| \ \rangle$.

- Les probabilités complexes d'amplitudes sont notées α et β, leur somme au carré vaut par conséquent 1 :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \ldots. \text{(I.1)}$$

La notation abstraite de Dirac pour l'état $|\psi\rangle$ peut conduire à différentes représentations mathématiques : l'état peut être représenté par une fonction $\psi(r, t)$ (formalisme des fonctions d'ondes et de la mécanique ondulatoire), ou par une matrice (notamment dans le cas d'espaces de dimensions finies), ou par les deux (matrice de fonctions). Dans notre espace à deux dimensions on peut utiliser une représentation matricielle [2] :

$$|0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \ldots. \text{(I.2)}$$

2.3. Vecteur Ket

Un élément quelconque, ou vecteur, de l'espace ξ est appelé « *vecteur Ket* », ou plus simplement « *Ket* ». On le note par le symbole | ⟩ en mettant à l'intérieur un signe distinctif permettant de caractériser le ket correspondant par rapport à tous les autres. On peut décomposer $|\psi\rangle$ dans la base des $|u_n\rangle$ [3] :

$$|\psi\rangle = \sum_{n=1}^{N} \psi_n . |u_n\rangle \ldots. \text{(I.3)}$$

Par convention $|\psi\rangle$ sera représenté par une matrice (ou vecteur colonne) contenant les composantes de $|\psi\rangle$ dans la base correspondante [3] :

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ . \\ . \\ . \\ \psi_N \end{pmatrix} = \begin{bmatrix} \psi_1 \\ \psi_2 \\ . \\ . \\ . \\ \psi_N \end{bmatrix} . (|u_n\rangle\,|u_n\rangle \ldots |u_n\rangle \ldots . \text{(I.4)}$$

2.4. Vecteur Bra

A tout « *vecteur Ket* » $|\psi\rangle$ de ε, on associera un vecteur dit « *vecteur Bra* », noté $\langle\varphi|$ .On peut décomposer$\langle\varphi|$ [3] :

$$\langle\varphi| = \sum_{n=1}^{N} \varphi_n . \langle u_n| \ldots . \text{(I.5)}$$

On représente aussi le « *Bra* » sous la forme d'une vecteur ligne, une suite de nombres (les composantes) rangés horizontalement [3] :

$$\langle\varphi| = \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ . \\ . \\ . \\ \varphi_N \end{pmatrix} = \begin{bmatrix} \langle u_1| \\ \langle u_2| \\ . \\ . \\ . \\ \langle u_N| \end{bmatrix} . [\varphi_1 \varphi_2 \ldots \varphi_N] \ldots . \text{(I.6)}$$

2.5. Bra –Ket composites

Deux « *espaces Hilbert* » V et W peuvent former un troisième espace V⊗W par un produit tensoriel. En mécanique quantique, cela sert à décrire les systèmes composites. Si un système est composé de deux sous-systèmes décrits respectivement par V et W, alors l'espace Hilbert de l'ensemble du système est le produit tensoriel des deux les espaces. (L'exception à cela est si les sous-systèmes sont réellement identiques particules. Dans ce cas, la situation est un peu plus compliquée) [4].

Si $|\psi\rangle$ est un « *Ket* » en V et $|\varphi\rangle$ est un « *Ket* » dans W, le produit tensoriel des deux « *Kets* » est un « *Ket* » dans V⊗W. Ceci est écrit de diverses manières :

$$\text{« } |\psi\rangle\,|\varphi\rangle \text{ ou } |\psi\rangle \otimes |\varphi\rangle \text{ ou } |\,\psi\varphi\,\rangle \text{ ou } |\,\psi, \varphi\,\rangle \text{ »} \ldots . \text{(I.7)}$$

3. Le qubit

3.1. Qubits et postulats quantiques

Il est temps maintenant de préciser les premiers postulats de la mécanique quantique.

3.3.1. Postulat de l'état d'un système quantique

La brique de base en théorie de l'information est le bit. La mécanique quantique nous enseigne qu'un tel système ayant deux états classiques possibles 0 et 1 peut également être dans une superposition de 0 et de 1.où, $\beta \epsilon$ C avec [5] :

$$|\alpha|^2 + |\beta|^2 = 1 \ldots . \text{(I.8)}$$

De façon plus abstraite, l'espace des états possibles d'un bit quantique (qubit) est donc la sphère unité de $C^{\{0,1\}}$, le C-espace vectoriel de dimension 2 engendré par $|0\rangle$ et $|1\rangle$ et muni de la norme euclidienne [5] :

Remarque :

- $|0\rangle$ et $|1\rangle$ sont simplement une base d'un espace vectoriel complexe de dimension 2. Ils correspondent à une mesure possible.
- On peut choisir n'importe quelle autre base de mesure, par exemple :

$$|+\rangle = (|0\rangle+|1\rangle)/\sqrt{2}$$

$$|-\rangle = (|0\rangle -|1\rangle)/\sqrt{2}$$

Etat d'un registre :

✓ L'état d'un seul qubit est un vecteur dans un espace à 2 dimensions [6] :

- l'un des 2 états de base : $|0\rangle$ ou $|1\rangle$
- ou, plus généralement, une superposition d'états de base :

$$\mathbf{|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle .... (I.9)}$$

Avec la probabilité (I.8)

✓ L'état d'un registre de 2 qubits est un vecteur dans un espace à 4 dimensions [6] :

- l'un des 4 états de base : $|00\rangle$, $|01\rangle$, $|10\rangle$ ou $|11\rangle$
- ou, plus généralement, une superposition d'états de base :

$$\mathbf{|\psi\rangle = a|00\rangle + b|01\rangle + g|10\rangle + d|11\rangle .... (I.10)}$$

Avec :

$$\mathbf{|a|^2 + |b|^2 + |g|^2 + |d|^2 = 1 .... (I.11)}$$

- Exemples :

- $|\psi\rangle = 1/2\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- $|\varphi\rangle = 1\sqrt{2}\ (|00\rangle + |11\rangle)$

✓ L'état d'un registre de Plusieurs qubits :

Plus généralement l'état $|\psi\rangle$ d'un registre de *n* bits quantiques est une superposition des 2^n états classiques possibles [5] :

Définition :

$$|\psi\rangle = \sum_{x\epsilon\{0,1\}^n} \alpha_x |x\rangle \ldots . \textbf{(I.12)}$$

Tel que :

$$\| |\psi\rangle \| = \sqrt[I]{\sum_{x\epsilon\{0,1\}^n} |\alpha_x|^2} \ldots . \textbf{(I.13)}$$

3.3.2. Postulat sur les grandeurs observables

A toute grandeur observable est associé un opérateur linéaire (hermétique) agissant dans l'espace des états ε. Dans les situations que nous considèrerons ces operateurs auront un ensemble discret de valeurs propres et d'états propres ; par exemple pour un observable **Ą** auquel est associé un opérateur A [1].

$$\exists\ \alpha_n \in \mathbf{C}\ \textbf{et}\ |\varphi_n\rangle \in \boldsymbol{\varepsilon},\ \text{tels que}\ \mathbf{A}|\varphi_n\rangle = \alpha_n|\varphi_n\rangle \ldots . \textbf{(I.14)}$$

Pour :

$$\mathbf{n = 1 \ldots n = dim(\varepsilon)}$$

Les états $|\varphi_n\rangle$ sont orthonormés et constituent une base dans ε :

$$\langle\varphi_n|\ \varphi_m\rangle = \delta_{nm} \ldots . \textbf{(I.15)}$$

$$\forall\ |\psi\rangle \in\ \varepsilon|\psi\rangle\ = \sum_n \alpha_{\,n}|\varphi_m\rangle \ldots . \textbf{(I.16)}$$

Avec :

$$\alpha_n = \langle\varphi_n|\psi\rangle \ldots . \textbf{(I.17)}$$

Dans la première équation δ_{nm}est le symbole de Kronecker défini par δ_{nm}= 1 si n = m et 0 sinon. Dans notre exemple du qubit les états $|0\rangle$ et $|1\rangle$ sont les états propres d'une grandeur observable. Si le système physique est un atome l'observable est l'énergie de

l'atome et les états |0⟩ et |1⟩ correspondent aux états |g⟩ et |e⟩ (état fondamental et premier état excité) de l'atome. Dans le cas où le système quantique est le photon l'observable est la polarisation qui peut prendre les deux états $|x\rangle$ et $|y\rangle$. Comme ces états forment une base dans l'espace des états du qubit, On a [1] :

$$\forall\, |\psi\rangle \in \varepsilon \quad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \ldots. \text{(I.18)}$$

Exemple :

Les opérateurs de projection (ou projecteurs) sur les états de base :

$$p_0 = |0\rangle\langle 0|,\ p_1 = |1\rangle\langle 1|$$

Sont tels que :

$$p_0|\psi\rangle = |0\rangle\langle 0||\psi\rangle = \alpha\,|0\rangle \text{ et } p_1\,|\psi\rangle = |1\rangle\langle 1||\psi\rangle = \beta|1\rangle$$

En représentation matricielle :

$$p_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } p_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

3.3.3. Postulat de la mesure

La mécanique quantique nous dit que si un système peut être dans deux états par exemple un bit dans l'état 0 ou 1 ; ou un chat vivant ou mort – alors ce système peut être dans une superposition de ces deux états. Or, dans la vie de tous, les jours nous observons rarement des superpositions de 0 et de 1 et encore moins des chats à la fois vivants et morts ! Une explication à cela : l'observation, aussi appelée mesure quantique, obéit à un postulat qui ne rend que les états classiques directement observables. Si un qubit dans l'état $\alpha|0\rangle + \beta\,|1\rangle$ est mesuré alors avec probabilité $|\alpha|^2$ la valeur 0 est observée et avec probabilité $|\beta|^2$ la valeur 1 est observée. De plus, la mesure projette l'état du qubit dans l'état observé, à savoir |0⟩ dans le premier cas et |1⟩ dans le second [5].

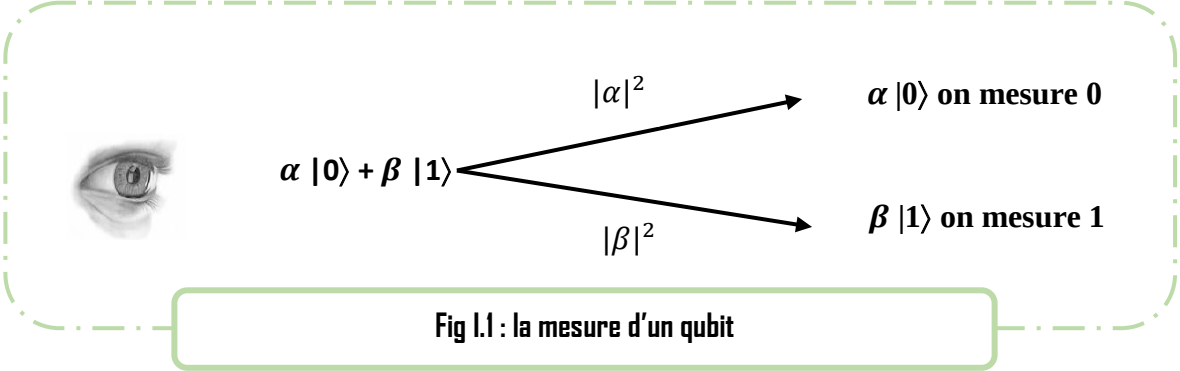

Fig I.1 : la mesure d'un qubit

3.3.4. Postulat de Système composé

L'état d'un registre classique dont on connait l'état des sous-registres est obtenu par simple concaténation de ces états : par exemple un registre de 3 bits dont les deux premiers sont dans l'état **01** et le troisième est dans l'état **1**, est dans l'état **011**. La composition des états quantiques s'obtient à l'aide du produit tensoriel [5] :

Définition :

Soit $|\psi_1\rangle$ l'état d'un registre de *n* qubits et $|\psi_2\rangle$ celui d'un registre de *m* qubits, l'état du registre composé de (*n* + *m*) qubits est :

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \text{.... (I.19)}$$

Avec $\cdot\otimes\cdot$ bilinéaire et :

$$\forall\, x \in \{0,1\}^n, \forall\, y \in \{0,1\}^m, |x\rangle \otimes |y\rangle = |xy\rangle \text{.... (I.20)}$$

L'état d'un registre composé d'un premier sous registre dans l'état $\sum_{x\epsilon\{0,1\}^n} \alpha_x|x\rangle$ et d'un second dans l'état $\sum_{y\epsilon\{0,1\}^n} \beta_y\,|y\rangle$ est donc :

$$\sum_{x\epsilon\{0,1\}^n, y\epsilon\{0,1\}^n} \alpha_x\beta_y|xy\rangle \text{.... (I.21)}$$

Le produit tensoriel "⊗" transforme deux vecteurs d'un espace vectoriel de dimension *n* en un vecteur d'un nouvel espace vectoriel de dimension n^2 [7] :

$$|x\rangle\otimes|y\rangle = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \\ x_2 \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \\ x_3 \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x1\,.\,y1 \\ x1\,.\,y2 \\ x1\,.\,y3 \\ x2\,.\,y1 \\ x2\,.\,y2 \\ x2\,.\,y3 \\ x3\,.\,y1 \\ x3\,.\,y2 \\ x3\,.\,y3 \end{pmatrix} \text{.... (I.22)}$$

Exemple [5] :

Dans les exemples qui suivent nous utilisons deux couleurs dans un but pédagogique pour mettre en évidence le premier registre (en vert) et le second (en noir).

$$|0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle - i|1\rangle}{\sqrt{2}} \otimes \frac{|00\rangle - |10\rangle}{\sqrt{2}} = \frac{|000\rangle \otimes i|010\rangle - i|100\rangle \otimes |110\rangle}{2}$$

3.2. Le qubit VS le bit [8]

Classique	Quantique
1 bit : 0 ou 1	**1 qubit :** $\alpha \|0\rangle + \beta \|1\rangle$ $\quad |\alpha|^2 + |\beta|^2 = 1$
N bit : 000…0 (0) 000…1 (1) 111…1 (2^n-1)	**N qubit :** $\sum_{i=0}^{2^n-1} c_i \|i\rangle$ $\sum_{i=0}^{2^n-1} \|c_i\|^2 = 1$ **Ex.** à 4 qubits : $\|7\rangle = \|0111\rangle$
Mesure : $b_1 b_2 \ldots . b_n \longrightarrow b_1 b_2 \ldots . b_n$	**Mesure :** $\sum_{i=0}^{2^n-1} c_i \|i\rangle \longrightarrow$ avec probabilité $\|c_i\|^2$

Tab I.1 : comparaison de qubit quantique VS le bit classique.

4. Intrication quantique

Deux systèmes sont dit séparés quand, étant éloignés, les observations faites sur l'un ne dépendent pas du tout de celles faites sur l'autre : il n'y a pas d'interaction.

Quand deux systèmes ne sont pas séparés, on dit qu'ils sont intriqués. La théorie quantique stipule qu'il existe des systèmes qui restent corrélés, même s'ils se trouvent suffisamment distants pour qu'aucune information ne puisse être transmise entre eux. C'est pour cela que l'on qualifie la théorie quantique comme une théorie non-locale car elle ne tient

pas compte de la localité. On retrouve cette notion dans la formalisation mathématique suivante [9].

Définition :

On dit qu'un état $|u\rangle$ est intriqué s'il n'existe pas d'états $|x\rangle$ et $|y\rangle$.

Tels que :

$$|\boldsymbol{u}\rangle = |\boldsymbol{x}\rangle \otimes |\boldsymbol{y}\rangle \text{ .... (I.23)}$$

5. Base de Bell

En effet, le vecteur $|\boldsymbol{\psi}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{00}\rangle + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{11}\rangle$ de notre exemple est un des quatre états intriqués prouvés par John Bell [22] dits états de Bell, ou de paires EPR (Einstein-Podolsky-Rosen), que l'on qualifie également de base de Bell :

$$|\boldsymbol{B_{00}}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{00}\rangle + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{11}\rangle.$$

$$|\boldsymbol{B_{01}}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{01}\rangle + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{10}\rangle.$$

$$|\boldsymbol{B_{10}}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{00}\rangle - \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{11}\rangle.$$

$$|\boldsymbol{B_{11}}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{01}\rangle + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|\mathbf{10}\rangle.$$

L'intrication est une ressource importante dans le traitement quantique de l'information. Elle joue un rôle important dans plusieurs protocoles pour la communication et la cryptographie quantique [18].

6. La cryptographie quantique

Le but de la cryptographie est la transmission d'un message d'un émetteur (Alice) vers un récepteur (Bernard), minimisant les risques qu'un espion puisse intercepter et décoder ce message. La cryptographie classique fait pour cela appel à des méthodes de codage sophistiquées, qui ne peuvent être «cassées» en un temps raisonnable compte tenu des moyens de calcul actuellement disponibles. La cryptographie quantique fonctionne sur un principe différent : elle permet à Alice et Bernard de s'assurer qu'aucun espion n'a intercepte leur message ! [10].

7. Protocole de téléportation

La téléportation quantique est un protocole de communications quantiques consistant à transférer l'état quantique d'un système vers un autre système similaire et séparé spatialement du premier en mettant à profit l'intrication quantique.

« Alice » et « Bob » partagent une paire EPR « b-c ». « Alice » reçoit une particule quantique « a » dans un état inconnu (qu'elle ne peut d'ailleurs déterminer) et la couple à son partenaire EPR « b ». Elle effectue une mesure collective sur l'ensemble « a-b » ainsi formé. Cette mesure a un effet immédiat sur la particule « c » de « Bob » (en raison de l'intrication « b-c »). L'état final de « c » dépend de l'état initial de « a » et du résultat de la mesure d'« Alice ». Elle communique classiquement ce résultat à « Bob » qui peut alors, par une transformation unitaire sur « c », reconstituer l'état initial de « a » [9].

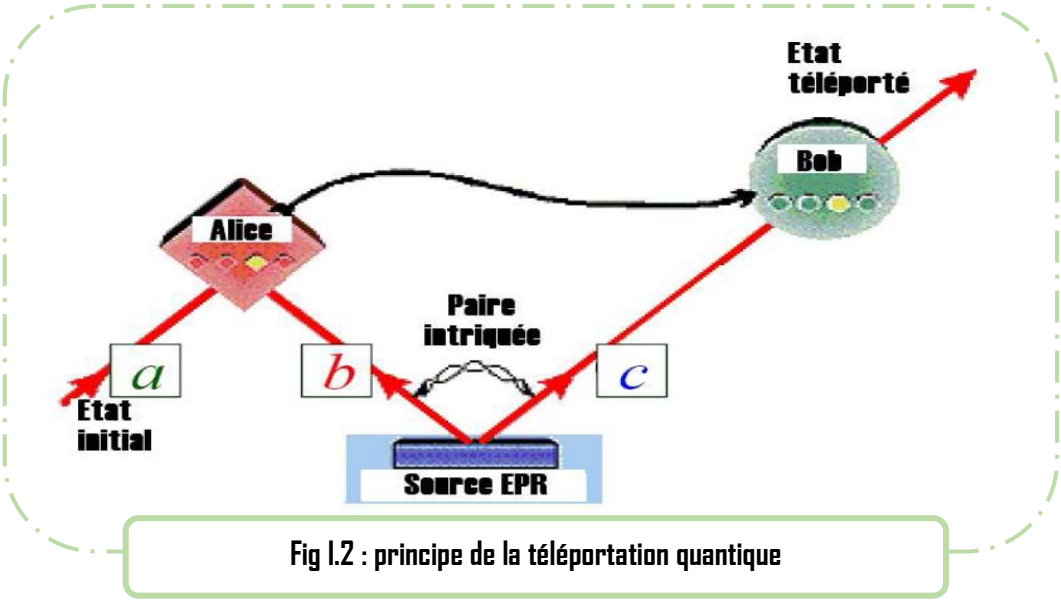

Fig I.2 : principe de la téléportation quantique

8. Conclusion

Dans ce chapitre, nous avons présenté les concepts de base reliés à l'informatique quantique ainsi que les postulats qui régissent la théorie associée. On a remarqué que cette discipline fait appel à plusieurs spécialités telles que la physique, les mathématiques et l'informatique. L'objectif visé par cette intégration de connaissances est la réalisation d'un calculateur quantique capable d'effectuer certains calculs plus rapidement qu'un ordinateur classique. Un exemple type est la factorisation des grands nombres entiers. Il s'agit d'un problème très difficile en termes de complexité algorithmique.